DEPARTMENT OF PERSONNEL & ADMINISTRATION	HIPAA Policy No.	7
	Current Effective Date	May 1, 2006
	Original Effective Date	May 1, 2006
HEALTH INSURANCE PORTABILITY AND ACCOUNTABILITY ACT	Approved by: Jeffrey C. Schutt Date: 4/25/06	
PASSWORD MANAGEMENT		

I. Purpose

To protect the confidentiality, integrity, and accessibility of Department of Personnel and Administration (DPA) computer systems and the data they contain through the use of passwords.

II. Policy

The HIPAA Security Rule requires covered entities to implement procedures to verify that a person (or entity) seeking access to electronic protected health information (ePHI) is the one claimed. It is common practice in the field of computer security to use passwords to authenticate the identity of a user when the user attempts to gain access to a file, application, or computer system. This practice has been adopted by DPA.

A. Creating a Password

Passwords must be hard to guess, but easy to remember. See the Procedures section below for guidance on how to create a good, strong password.

B. Security Risks

1. Writing down passwords
   Use easy-to-remember passwords so that you do not have to write them down or otherwise record them (*e.g.,* store them in a PDA). Writing down or recording a password is a serious security risk because anyone who has access to or can see (purposely or unintentionally) the writing or recording of the password can potentially get into files, applications, or computer systems.

2. Sharing passwords
   a. Passwords must not be shared with anyone, including family, friends, co-workers, and supervisors, for the following reasons:

      - Sharing passwords is a serious security risk because it compromises the ability to authenticate the identity of a user. The ability to identify a user is essential if users are to be held accountable for their activities.
      - A user who shares a password with one person is more likely to share the password with others, as well, than a user who keeps the password secret.
      - Once a password is shared, the user with whom the password is identified no longer has control over its use, including access to files, applications, and computer systems.
      - The person to whom a password is revealed may not keep it secret.

   b. Passwords must not be shared even with IT personnel, including help desk technicians and system administrators, and IT personnel must not ask users for their passwords.

C. Changing Your Password

Passwords must be changed every 30 days. The system will prompt you when it is time to change your password.

III. Procedures

A. Creating a Password

1. Passwords must be at least 9 characters long, and include both numbers and letters. Combining upper and lower case letters, numbers, and symbols (*e.g.,* #, %, ?) is even better.

2. Use as many different characters as possible.

3. Avoid sequences (*e.g.,* 12345 or qrstu) or repeating characters (*e.g.,* aaeeiioouu)

4. Do not use any of the following:

   - Personal information that someone else is likely to know (such as your child's name) or likely to be able to figure out (such as your date of birth)
   - Words that may appear in any dictionary (or other reference book) in any language, even if you spell them backwards (except that words may be used as part of a combination, as shown in paragraph 5, below
   - Geographical or biographical names, or names of fictional characters
   - Passwords that have been used as examples in discussions about passwords (such as this policy or articles on the Internet)
   - Common words with letters replaced by numbers or symbols (*e.g.,* h3llo, he!!o)
   - Old passwords (passwords that you have already used)

5. Methods for creating a password

   - Think of a sentence or phrase that you can easily remember. Take the first letter of each word and mix in some numbers and symbols to create your password. For example, "Raindrops keep falling on my head" could be RKF63omH!
   - Use an intentionally misspelled word with numbers and symbols added. For example, Choch-L1T.
   - Add numbers and symbols to a word. For example, #Chocolate74.

B. Urgent Situations

If access is needed to the files or computer system of a user who is not available (*e.g.,* on vacation), IT personnel will respond promptly (usually within ten (10) minutes) if a supervisor or manager contacts the help desk and indicates that the situation is urgent.

IV. Definitions/Abbreviations

Access means the ability or the means necessary to read, write, modify, or communicate data/information or otherwise use any IT system resource. Access must be controlled to ensure that private information remains private.

Confidentiality means that data or information is not made available or disclosed to unauthorized persons or processes.

Integrity means that data or information have not been altered or destroyed in an unauthorized manner.

Password means confidential authentication information composed of a string of characters; a secret word or phrase that one uses to gain admittance or access to information.

V. Revision History

Date	Description
May 1, 2006	Original document

VI. References/Citations

Security Rule	
45 CFR 164.308(a)(4)	Information Access Management
45 CFR 164.308(a)(5)(ii)ID)	Password Management
45 CFR 164.312(a)(2)(1)	Unique User Identification
45 CFR 164.312(c)	Integrity
45 CFR 164.312(d)	Person or Entity Authentication